SECURITY RISK ASSESSMENT METHODOLOGY FOR BIOSCIENCE FACILITIES

Natalie Barnett[1], Jennifer Gaudioso, Reynolds M. Salerno

Sandia National Laboratories[2]
P. O. Box 5800, MS 1371
Albuquerque, NM 87185

ABSTRACT

Protecting the United States against bioterrorism requires a multifaceted approach; one of these facets is biological weapons nonproliferation (BWNP). Securing dangerous pathogens that are held in legitimate bioscience facilities worldwide can be effective BWNP strategy. In order to apply adequate security without wasteful over-allocation of resources, a risk assessment of those facilities holding the most dangerous pathogens should be conducted. Many of the fundamental principles of security risk assessment apply to bioscience facilities. Assets must be identified; the consequences of loss of those assets must be established; and the threat environment must be analyzed. However, what is missing from traditional security risk assessment methodologies is an understanding the nature of dangerous pathogens and toxins, and the attractiveness these assets might pose for an adversary. A security risk assessment methodology specifically designed for biological facilities is being developed at Sandia National Laboratories. This methodology provides a means of prioritizing the bioscience facility risk by evaluating a variety of attributes associated with the facility's assets and threat environment. This prioritization may then be used as a guide to preferentially allocate funding towards securing those materials at the highest risk of diversion.

[1] Corresponding author: phone: (505) 284-6615, email: nbarnet@sandia.gov
[2] Sandia is a multiprogram laboratory operated by Sandia Corporation, a Lockheed Martin Company, for the United States Department of Energy's National Nuclear Security Administration under contract DE-AC04-94AL85000.

INTRODUCTION

The threat of dangerous biological materials being used to kill or disable humans, livestock, or crops, and the strategies used to address this possibility, have changed over the years. Historically, the threat was one of biological warfare, waged by States in times of conflict. More recently, the concern has grown to include the threat of bioterrorism—acts waged by nonstate actors against military and civilian targets alike.

Biological weapons nonproliferation (BWNP) programs are designed to stop the acquisition, development and use of biological agents as weapons. Biological weapons nonproliferation efforts have, until recently, been largely focused on keeping States from developing offensive biological warfare capability, or sharing this capability with other States, and transitioning institutions and scientists formerly involved in weapons programs to peaceful research endeavors. States were considered to be the only category of adversary capable of developing these weapons because of the need for large facilities, sophisticated equipment, and highly trained personnel. These factors are changing rapidly as the biotechnology revolution is sweeping the world. Automation and "kits" have reduced the level of expertise necessary to accomplish a variety of tasks associated with growth and strain selection, and the expansion of the industry has increased the availability of necessary facilities, equipment, and personnel. Now, nonstate actors, with fewer resources and different objectives, may be in a position to acquire, develop, and use biological weapons.

Laboratories, culture collections, and other legitimate bioscience facilities located around the world have viable, virulent strains of dangerous biological agents in their possession. These biological agents are well characterized and purified, in contrast to the biological agents found in the environment, which are of lesser known quality and suitability for use as a biological weapon. Some of the biological agents that are found in these legitimate facilities might therefore be an attractive target for acquisition by an adversary interested in pursuing biological terrorism. Securing those biological agents that would make the most effective biological weapons would limit the risk of bioterrorism by reducing the availability of the most suitable materials. A risk assessment methodology designed to evaluate biological materials as weapons[1,2], and the capabilities of those interested in acquiring them, should be used to determine which biological materials, in which facilities worldwide, should be secured.

Historically, security risk assessments have not been oriented towards biological assets, or towards the risk of malicious acquisition of dangerous biological materials from legitimate facilities. However, many of the fundamental security principles used to assess the risk of malicious diversion of other types of assets, in other types of facilities, are applicable to biological facilities. Assets must be identified; the consequences of loss of those assets must be established; and potential adversaries and the threat they may pose must be analyzed. What is missing from traditional security risk assessment methodologies is an understanding of the nature of dangerous pathogens and toxins, and the attractiveness these assets pose for an adversary determined to perpetrate an act of bioterrorism. A security risk assessment methodology specifically designed for biological facilities and their biological assets is under development at Sandia National Laboratories.

RISK ASSESSMENT

The Department of Homeland Security (DHS) has recently acknowledged the need to "manage risk at the homeland security level… Each threat must be weighed, therefore, along with consequence and vulnerabilities." Secretary Chertoff has recognized the need to prioritize risks, stating "the plain truth is that there is no 100-percent solution. We cannot protect every person in every place at every moment. We cannot look in every container and every box. What we can do is use intelligent risk-based analysis, advanced technology and enhanced resources to manage risk."[3]

The Government Accountability Office also endorses a risk management approach to security. They recommend an approach which 1) establishes which assets should be protected against which threats, and 2) ensures that the amount of protection provided to a specific asset, and the cost for that protection, is proportional to the risk of the theft or destruction of that asset.[4]

Taking a risk management approach to protecting dangerous pathogens and toxins from malicious acquisition and use begins by identifying which assets (e.g. biological agents) to protect, and which facilities have these assets. This preliminary screening will reduce the number of facilities that should be considered for a more comprehensive risk assessment. Once those facilities that hold the most attractive biological assets are identified, the threat to those facilities, and the vulnerabilities of those facilities, can be evaluated, i.e. their risk may be assessed. Risk reduction strategies can then be applied to reduce those risks that are significant enough to warrant an investment in security measures and/or consequence mitigation techniques. Risk reduction should be pursued internationally so that acquisition of dangerous biological materials will not simply be pursued through the weakest international link.

The risk that a particular facility may be targeted for acquisition of dangerous biological materials may be expressed as a relationship between the "threat potential" posed by an adversary, and the "consequences" of acquisition and subsequent use of the material as a weapon. These risks can be prioritized by scenario; scenarios include an adversary, an asset (target), and an action (e.g. theft and use, or sabotage).

Many elements of this analysis rely heavily on expert judgment. It is not possible to predict what an adversary will do, when they will do it, where, or even if they will pursue a particular action. However, there are ways to address these questions using a structured methodology that provides consistency, traceability, and transparency. These features provide the appropriate authorities with a basis for discussion and decision making.

A bioscience facility risk assessment begins by identifying and cataloging the assets held at the facility based on the impacts associated with their theft or sabotage. If the consequences of loss are significant enough to outweigh the expense of countermeasures, those assets should be incorporated into theft and/or sabotage scenarios for evaluation, otherwise, the assessment may stop with no further action being taken. This is a rough baseline assessment that is often influenced by the risk tolerance of the institution, the information that is readily available regarding the nature of the assets held at the facility, and regulations the facility must follow.

If further risk assessment is justified, an evaluation of the threat environment of the facility should be conducted to provide information on the adversaries that are relevant to the facility. The intelligence community, local law enforcement, site security, and facility management

personnel should be asked about any extremist, terrorist, or criminal activity in the area, union activity, acts by disgruntled employees, and about any other sources of tension in the area.

Once the potential adversaries have been evaluated, the facility should be characterized to ascertain the potential opportunities for an adversary to acquire or destroy the asset of interest. The analyst should understand the mission, operations, processes, policies and procedures of the facility. The location of the assets, potential pathways for access, and existing security features must also be established, as well as any vulnerabilities or gaps in the existing security that would allow an unacceptable risk to materialize.

Motive, Means and Opportunity

The main premise of this methodology is that the adversary's motive, means and opportunity are critical elements in assessing the risk of an asset being targeted for acquisition. The adversary's motive is based on an assessment of whether or not, and to what degree, theft and use of the asset would meet a particular adversary's objective. An adversary's means is based on an assessment of technical skills, operational knowledge, and tools. The adversary's opportunity is determined by an assessment of how difficult or easy it would be for the adversary to gain access to the asset; thus, opportunity is related to whether the adversary is an "insider," who has authorized access to the facility, or an "outsider," who does not.

We assess an adversary's motive, means, and opportunity according to a set of adversary classes with generalized characteristics. The assumptions that underlie these adversary classes will influence outcomes of the risk assessment and are a significant contributor to the uncertainty inherent in this form of analysis. However, generalized adversary classes provide a useful starting point for the analysis. In order to increase the relevance of these adversary classes to the facility being analyzed, the local threat environment within which a particular facility exists should be evaluated. The local threat environment data should be incorporated into the adversary class descriptions and used to inform the analysis of adversary motive, means and opportunity. Interviews with site security personnel, local law enforcement and the intelligence community should be conducted to establish the level of activity of various adversary groups in the area and the potential threat posed to the facility. Questions should focus on the nature, timetable and proximity to the facility of any reported activity by terrorists, extremists or other protesters, psychotic individuals, and criminals.

In assessing the motive of an adversary, we use the adversary classes of terrorist, psychotic, extremist, and criminal, and their assumed objectives, as the basis for the analysis. The objective of the terrorist adversary class is to cause mass casualties, an economic crisis, and/or widespread fear based on an ideological or emotion-based rationale. Psychotic individuals, as an adversary class, may also pose a significant threat and have motivations that may be convoluted and perhaps pathological because of a mental or behavioral disorder. The extremist adversary class is generally interested in making a political statement or expressing protest against programs for ecological, political, economic or other reasons, and may destroy property or release animals. The objective of the extremist adversary class is not assumed to be fulfilled by stealing or releasing biological materials into the environment, but their acts may inadvertently cause a release of pathogens into the environment by releasing contaminated animals. Criminals are generally motivated by financial gain.

If an adversary chooses bioterrorism as a tactic for meeting their objective, the choice of biological material will be a critical element in their attack plan. If the adversary is interested in

conducting an act of biological terrorism that will result in a high number of deaths, for instance, then the biological agent must have certain characteristics that make it usable as a weapon. These characteristics might include environmental stability, to survive the growth, storage, dissemination and contamination processes, and the proper disease-causing qualities to incur the high fatality rate the adversary desires.

We use the term "weaponization potential" to describe the characteristics of a biological agent that dictate the ease or difficulty with which it may be turned into, and deployed as, a biological weapon. The consequences that could be incurred as a result of deploying a biological weapon include death, illness, economic and psychological impacts. The relationship between consequences and weaponization potential influences the assessment of how attractive the pathogen or toxin is to an adversary who is intent on conducting an act of bioterrorism.

For the purposes of this analysis, weaponization potential consists of three factors: acquisition, production, and dissemination. These criteria can be broken down into sub-criteria to facilitate a systematic analysis. An adversary may acquire biological agents by isolating material from the environment, or stealing the material from a laboratory, culture collection or other legitimate facility. Environmental sources of biological agents include endemic areas and outbreaks sites. The ability to successfully isolate biological agents from the environmental depends on the adversary knowing where to collect the agent, how to identify the source, how to select a virulent strain and upon the availability of appropriate laboratory protocols within the open literature. In addition to these traditional acquisition pathways, advances in biotechnology have opened up another, more challenging, avenue to acquisition: chemical synthesis and genetic engineering. Some viruses have been synthesized in legitimate laboratories and bacterial agents could be created through the addition of virulence plasmids to a vaccine strain.

Once the agent of choice is acquired, the adversary must be able to produce a suitable amount of the agent in the appropriate form for it to be effectively used as a weapon. The degree of difficulty associated with this process influences both agent selection and the dissemination scenario, which ultimately determine the potential consequences. For instance, there is a great deal of variation in the required technical skills associated with amplifying an agent, producing quantities of liquid agent, and producing lyophilized agent.

Some agents require less sophisticated dissemination scenarios and thus simpler production protocols. The chosen mode of dissemination of a biological weapon depends on the effective routes of exposure for a particular pathogen or toxin. Pathogens and toxins may pass through the skin (typically through an abrasion), be inhaled, ingested orally, or transmitted through a vector. The mode of dissemination is an important factor in the complexity of the adversary's bioterror operation.

Not all biological agents are equally stable over time, and the use of preservatives or other stabilizers might be required. If a biological weapon preparation is not able to be stored until the optimal time of use without losing its efficacy, it may be less appealing to the adversary. An adversary must also consider the stability of an agent during and after dissemination. Stability can be affected by humidity, pH, temperature, chlorination, and ultraviolet radiation, among other factors.

Moreover, covert biological weapons activities require adequate containment and safety measures to prevent accidental release or exposure of the workers; a biosafety accident could result in the detection of the program.

This risk assessment methodology assumes that the selection of a particular biological material selection for use in a weapon is dependent not only upon the weaponization potential, but also upon the consequences that the biological agent could have on the target population. Consequences may be evaluated in terms of the health impacts on humans, animals or crops, economic impacts, social or psychological impacts, and operational impacts on a facility.

The effect of a biological attack on the health of the target population is influenced by: how easily the agent is transmitted (contagiousness), the percentage of those exposed who contract the disease and the resulting severity of disease (morbidity), the percentage of those exposed who will die (mortality), and the potential for the disease to become endemic (causing health or economic impacts).

A biological attack on humans or agriculture could result in varying degrees of anxiety, panic and social disruption. The degree to which a biological attack influences the behavior and psychological well being of those experiencing the consequences of such an attack may be an important feature in the choice of biological material for certain adversaries.

There will be direct economic impacts associated with any biological attack in the form of clean-up costs. There are likely to be a variety of less easily estimated secondary impacts, including those that affect the travel industry, the agricultural industry through new export controls, long-term medical care, etc.

Other facility assets should also be considered during the risk assessment. For instance, security information, and the systems that maintain this information, may be targeted to facilitate gaining access to dangerous biological materials. In addition, there are other assets at the facility, either structural or operational (e.g. experimental data or materials, animals, information systems, or others), that may be targeted for sabotage by political extremists, disgruntled employees, etc., which should be assessed as well.

The threat that an adversary presents to a facility is not only dictated by the assets the facility holds, and the adversary's motive for obtaining them, but also by whether the potential adversary has the means to acquire and use these assets in a manner consistent with the adversary's objective. The adversary needs adequate technical skills, operational knowledge and tools to conduct an act of bioterrorism. Some adversaries will be better suited than others to successfully execute such an attack and should be ranked accordingly.

The means of the adversary classes that are used in this analysis, like their motivations, are based on a generalized set of characteristics, and are subject to the same uncertainties. Terrorist groups are assumed to be well funded. Terrorist groups are generally well equipped, trained, and able to rehearse the attack. They have access to, and the skill to utilize, significant explosives and arms. Terrorist groups may be highly organized, are violent, and willing to die. Individual terrorists are not as well equipped, but may still be capable of killing or injuring a number of guards or other individuals; they are assumed to have the tools necessary to overcome most access control systems. Psychotic individuals may also pose a threat. These individuals may be armed with a handgun, and may be violent, but are typically unwilling to risk death. Extremists may operate individually or in groups. Their usual tactics are to march, picket, or commit violence against an institution. Extremists are assumed to have general information about the facility, but not specific information about the location of the assets or the facility's protection systems. They are possibly armed with a handgun, but are not homicidal (however collateral loss of human life is possible in the event arson is employed), and are not willing to risk death. The criminal is

assumed to act alone and willing to use weapons and hand tools to achieve his/her objective. In extreme cases, this adversary could be affiliated with organized crime.

Once the motive and the means of the adversary are assessed, the adversary's opportunity to acquire the asset needs to be evaluated. We assess the adversary's opportunity to conduct a malicious act by evaluating the adversary's access and proximity to the asset. On a global level, the opportunity to acquire biological agents from legitimate facilities is influenced by the number of facilities that have the agent. On a local level, the opportunity of the adversary is assessed by evaluating the threat environment of the facility.

By definition, insiders are always an element of the threat environment and should be evaluated based on the level of access they have to the asset of concern. Other factors, such as an elevated level of hostility towards the facility management, should be incorporated into the analysis of the insider threat as well. The insider may have various levels of access to the asset, affecting their opportunity to commit the act. For biological materials, full access is often provided to those who regularly work in the laboratory; visiting laboratory personnel may have escorted access; those who work in offices adjacent to the laboratory areas may have building access; and there may be those who have site access only, including invited trades professionals, delivery personnel or other service personnel authorized to be on site on an irregular basis.

We assume that insiders will act covertly and abort any theft or sabotage attempt to avoid identification; they also have the opportunity to choose the best time to commit a malevolent act. When access to the asset is limited to those who are technically qualified, the insider with full access is assessed to have the opportunity and the means to acquire and use (or sabotage) the agent. Insiders with full access to biological materials are usually scientists and technicians who have a high level of technical training and sophistication. Thus, they often have all of the means at their disposal to successfully acquire and deploy a biological agent as a weapon. Restricted insiders may have considerably less opportunity to conduct a malicious act and may have inadequate means of gaining access to the asset.

Outsiders, by definition, do not have authorized access to the facility's assets, but as an adversary class they are not restricted to covert actions. Outsiders should be evaluated based on site-specific information.

The motive, means, and opportunity of an adversary to execute a particular scenario should be assessed for those assets at a facility that have a high consequence of loss. Scenarios should incorporate an asset, an adversary, and an act (e.g. a terrorist outsider stealing *Bacillus anthracis* and using it as a weapon). Each scenario that is evaluated can be plotted on a risk graph similar to that shown in Figure 1. Once all of the scenarios of interest have been examined, a picture of relative risk will emerge.

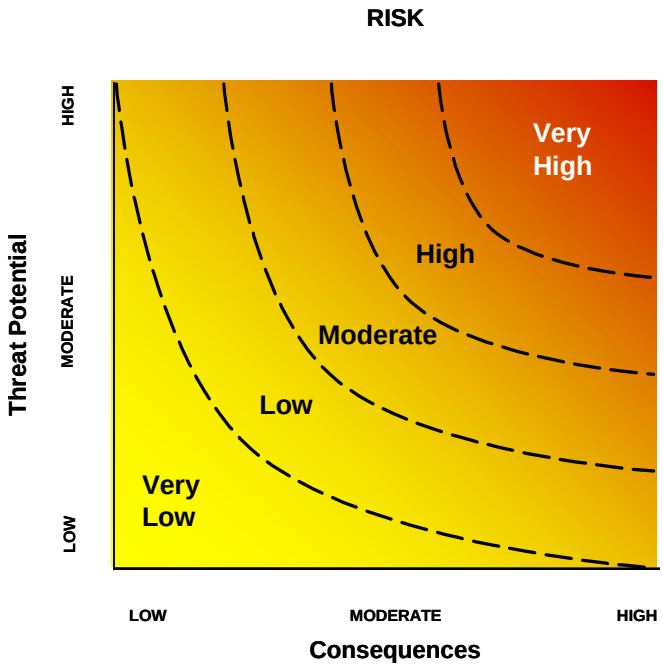

Figure 1. Risk Graph

Risk Mitigation

It is important to focus on the highest priority risks and to invest in risk reduction in a manner commensurate with reasonable expectations of what can be achieved. Risk cannot be eliminated and risk reduction efforts quickly reach a point of diminished returns for the investment made. Thus, some amount of residual risk will always remain. This is the level of risk that must be accepted. Decision makers must understand their level of risk tolerance, or risk aversion, and apply their resources for risk mitigation accordingly.

A primary objective of this risk assessment methodology is to help decision makers understand the risks associated with various facilities worldwide that possess dangerous biological materials. Risks must first be identified and ranked. Decision makers must then decide which risks to mitigate and how. *Which* risks are mitigated is driven by how highly the risk is ranked; *how* the risk is mitigated is driven by the adversary and the asset involved. One way to mitigate risk is by reducing the threat potential an adversary poses through security measures. Another way to reduce risk is through consequence reduction using medical countermeasures such as early detection, diagnosis and treatment. Threat reduction and consequence mitigation may be achieved independently or in conjunction depending on the resources available and the technical hurdles involved. See Figure 2.

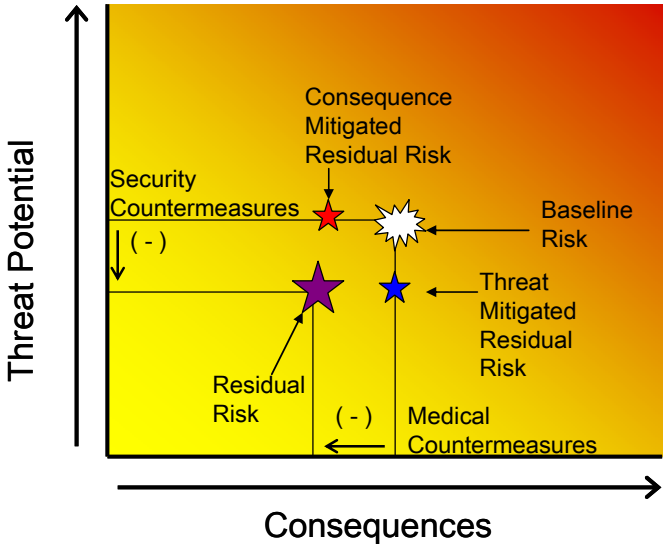

Figure 2. Risk Mitigation

Preventative strategies associated with biological weapons nonproliferation, in the context of illicit acquisition of dangerous biological materials from legitimate laboratories, may involve applying security countermeasures at those facilities facing the highest risks. By limiting an adversary's opportunity to act (and reducing the number of adversaries with the means to act), a facility may reduce the threat it faces. Because most biological materials are found in nature, deterrence may be the most prudent approach for the majority of facilities that hold biological assets. The objective should be to invest the minimum amount of resources necessary to compel adversaries to acquire the materials they need from nature rather than from the facility's biological stocks.

In general, insiders pose the greatest threat because of their technical knowledge, operational understanding and opportunity to acquire or destroy an asset. Insiders are also the most difficult to address with security measures. One of the most effective means of limiting the insider threat is to limit the opportunity of the insider to covertly acquire the asset; this may be done by restricting the number of insiders with access to the asset of concern. Restricting access to authorized insiders can be achieved through physical controls, as well as through personnel screening. Once the population of insiders is reduced to those who have a legitimate need to access the asset of concern, additional procedural controls may be established to limit the opportunity of these insiders to covertly acquire or destroy the asset. These control measures may be implemented through material handling and control, transport security, information security and program management.

If the risk assessment shows an outsider to be an adversary that presents a threat to the facility, the focus of the security measures applied to this threat should shift from controlling and screening personnel, to physical security systems designed to detect intrusion and to communicate intrusions to response forces. Personnel screening also supports mitigation of the

outsider threat by reducing opportunities for collusion between an insider and an outsider and by controlling visitor access. Material handling and control, information security, transport security, and information security measures are also useful for mitigating the outsider threat.

SUMMARY

In order to balance the allocation of national resources towards reducing the risk of biological terrorism, it is important to understand how biological weapons nonproliferation efforts contribute to protecting the United States. Mechanisms for preventing the use of biological weapons often have been difficult to establish because of the dual use nature of biological materials. However, one facet of the risk of biological weapons proliferation can be addressed by reducing the threat of illicit acquisition of dangerous biological material from legitimate bioscience facilities. A risk assessment process specifically designed to address biological material acquisition and use should be applied and the results used by policy makers and facility managers to determine what assets in which facilities require protection, who the assets should be protected from, and the consequences of a protection failure. Risk assessment is a critical first step because failing to adequately protect an asset could allow an adversary to successfully execute a malevolent act, while overprotecting a nonessential asset would waste limited resources.

APPENDIX

For the purposes of this paper, the following definitions apply:

Facility: Any legitimate laboratory, culture collection facility, etc. that holds dangerous pathogens or toxins of concern for some period of time.

Facility Risk: An expression of the relationship between the threat potential and consequences for a particular scenario.

> Example scenario: theft and subsequent use of biological material as a weapon by a terrorist.

Threat Potential: An estimate of the degree to which a particular adversary is willing and able to execute a particular event.

Consequences: An estimate of the magnitude of a successfully executed scenario in deaths, illness, economic loss, and/or operational impacts.

NOTE: Consequences will vary depending on the asset and action taken. Deaths, illness, and economic loss may be impacts on a target population directly attributable to theft and use of biological material as a weapon. Operational impacts may be felt at a particular facility if indirect assets are attacked, through sabotage, such as the facility, or facility operational or information systems.

REFERENCES

[1] Arturo Casadevall and Liise-anne Pirofski "The weapon potential of a microbe," Trends in Microbiology, 12(6), 2004, 259-263.
[2] Jennifer Gaudioso and Reynolds M. Salerno "Biosecurity and Research: Minimizing Adverse Impacts," Science, 304, 2004, 687.
[3] Remarks for Secretary Michael Chertoff U.S. Department of Homeland Security George Washington University Homeland Security Policy Institute, Washington, D.C., George Washington University, Homeland Security Policy Institute, March 16, 2005.
[4] US GAO, *Homeland Security: A Risk Management Approach Can Guide Preparedness Efforts*, GAO-02-208T (Washington, DC: October 2001). Also see US GAO, *Combating Bioterrorism: Actions Needed to Improve Security at Plum Island Animal Disease Center*, GAO-03-847, (Washington, DC: September 2003).